Private information in public spaces: Facial recognition in the times of smart urban governance

Juliana NOVAES,
University of Sao Paulo, Sao Paulo, Brazil
juliana.novaes.camargo@usp.br

Abstract

Cities are the stage of a curious phenomenon in which people feel at the same time at home and like complete strangers. A city provides simultaneously the familiarity of its residents concerning places and people and the possibility of living in relative anonymity. However, the last few decades have been accompanied by an increase in the use of information and communication technologies in the infrastructure and functioning of urban centers around the world. There has been a move towards the development of the commercial ecosystem of so-called smart cities, with the public administration increasingly partnering with private corporations to offer solutions in public services that involve the processing of personal data from citizens. **Objectives:** This paper aims to discuss the new dilemmas that arrive with the growth of surveillance technologies applied to urban centers and the increasing participation of the private sector in the processing of data whose origin lies within public services. **Prior work**: In order to accomplish so, this article analyzes this phenomenon from a capitalism surveillance framework perspective, in light of international data protection standards and with a primary focus on the analysis of the processing of citizens' data in the provision of public services **Approach:** The main approaches used are literature review and case studies. The first section will be dedicated to the discussion about the concept of "smart cities"; the second section will bring up the study of three cases about the implementation of facial recognition in the public transport system of the city of Sao Paulo; and the third and fourth sections are dedicated to the analysis of the legitimacy, risks, political and social implications of this type of surveillance practice. **Results:** As a result, this paper points to some of the issues that arise with the implementation of surveillance technologies in public services, such as the invasions of individuals' rights of privacy and freedom of expression. **Implications**: The study offers an opportunity for researchers and policymakers to have a perspective on how these practical cases reflect some of the academic discussions around surveillance in smart cities. **Value:** This paper, therefore, offers an original analysis of three existing cases and their insertion into a broader discussion of surveillance in urban centers and some of the risks involved.

Keywords: facial recognition, personal data, public services, surveillance, smart cities.

1. Introduction

Cities are a stage for a curious phenomenon in which people feel, at the same time, at home and as complete strangers. That is, a city offers, simultaneously, the familiarity of its residents regarding places and people and the possibility of circulating in relative anonymity [1].

However, the last few decades were accompanied by an increase in the use of information and communication technologies in the infrastructure and functioning of urban centers around the world [2]. Along with the fast development of the commercial ecosystem of the so-called smart cities, the public administration has progressively embraced digital mechanisms for processing personal data in its public services [1].

In the city of Sao Paulo, for example, three initiatives involving partnerships between the public and private sector were conducted, focused on implementing facial recognition technologies in the public transportation system.

This phenomenon implies a series of discussions about legitimacy in the processing of biometric data, given that the very nature of the public service provision does not allow for unrestricted consent from citizens concerning the use of their personal information.

Furthermore, the growing wave of public-private partnerships gives light to a debate about the limits of using personal data whose origin derives from services of public nature. Given this context, the present article intends to provoke reflections concerning some of these dilemmas, in the light of international standards of data protection, with focus on the analysis of social and political consequences of processing citizens' biometric data through the provision of public services.

Therefore, the first section will be dedicated to the discussion about the concept of smart cities; the second section will bring the study of three cases regarding the implementation of facial recognition in the transportation system of Sao Paulo; and the third and fourth sections are dedicated to the analysis of legitimacy, risks and political and social implications of surveillance practices conducted in partnership between the public and private sector.

2. Smart cities: An obscure concept

Globally, the movement of smart cities has grown steadily, with great speculations being made by the private sector around the potential for profit coming from this trend [1]. Efforts are being positioned for the advancement of technologies considered "smart" and this is done not only through the entrance of companies in the sector, but also by the very creation and modulation of this market [1].

Yet, all speculation about smart cities is still a foggy territory, given that not even its concept has been defined. The term is marked by a pluralism of definitions so that there is no consensus between the authors on this[2]. The expression is part of a contemporary conception regarding the development and management of urban centers using technology [3].

There are, nonetheless, some points in common that unite these different visions. In broader terms, smart cities relate to the creation of relationships between technology and society. In other words, it refers mostly to a vision of urban life and infrastructures that includes communication and information technologies [4].

Big cities present various challenges in topics such as security, housing, transportation, energy, supply, and communication. Thus, the justification for the integration of technology in its governance is based on the progressive growth of urban centers around the world and the necessity of optimization and efficiency in management [5].

Thus, the main element that surrounds the existence of smart cities is the ethos of technological innovation to promote solutions for governance and development of urban spaces [2]. It is, therefore, an initiative motivated by using technology to reach a new paradigm of communication through computational resources for informational integration and automation in the context of cities [5].

Some authors track the first appearances of the term smart cities in media vehicles to an optimistic discourse from the private sector towards a futuristic and efficient notion of urban centers [4]. Companies have a predominant role as disseminators of the discourse about smart cities and their benefits, a context in which the private sector would have a relevant role [4].

There is also an intrinsic relationship between data and smart cities. The idea of smart cities in general involves a vision of transforming the governance of urban centers through the massive production of data, which offers greater sophistication towards the understanding of how cities work [2]. In this sense, the use of big data for integration and analysis of a complex system becomes a major factor of influence for urban administration [6].

In other words, the great paradigm present in smart cities is the use of technology to build an idea of the urban center as a set of nodes in a connected network [1]. Nevertheless, the use of data to produce analysis about the functioning of urban centers is not an innovation brought by smart cities. Large data sets, such as national censuses and government records, have long been produced. However, before the massification of data-driven technologies, information about dynamic aspects of a city and its citizens were only incidentally collected to create public policy and this was usually done in a centralized manner, in the long run, or on a non-continuous basis [7].

The smart city, in this way, represents a paradigm shift to the volume and control of information generated from infrastructures, services, and civic spaces [1]. The proliferation of new forms of data processing offers a great opportunity for understanding urban processes, providing new ways to analyze, visualize and understand the social and spatial configuration of urban governance and economic development [8]. In this context, data is the reason for the existence of this new paradigm of urban governance.

Another key point in the development of smart cities is associated with the growth of inter-organizational partnerships and alliances between private and public entities [8]. The large flow of capital involved in this type of partnership is one of the factors that encourage the dissemination of the discourse around smart cities and, consequently, its appeal [9].

3. Facial recognition in the transportation system of the city of São Paulo

In Brazil and most Western countries, the provision of public services stems from a state duty to meet certain needs of society through the offer of essential services [10]. Ten principles govern the provision of public services in Brazil [11] and the following are highlighted for this study: the supremacy of public interest; universality; impersonality, resulting in the inadmissibility of discrimination between users; and transparency.

Due to its essentiality, public transport is a social right contained in the constitution, and its obligation of fulfillment is attributed to the state. This provision, in turn, can be carried out by state itself or through partnerships with the private sector, so that the public service providers can in practice be public or private entities [10].

This possibility of private agents having a role in the provision of public services facilitates the development of smart city initiatives in Brazil. The motivations that govern smart city initiatives are generally of an economic and political nature and are tied to the objective of transforming the urban space through actions linked to entrepreneurship [1]. This type of initiative usually requires extensive collaboration between public and private agents. The three cases mentioned illustrate this phenomenon, as they involve public-private partnerships within the context of public services.

In Case I, Line 4 of the Sao Paulo subway is an example in which the public transport service was delegated to a private agent. Line 4 operates through a concession, a modality in which the state transfers the management of the service to a private agent for a specified time, but not its ownership, which remains with the State of Sao Paulo. In this sense, there is no conversion of the public service to the private regime, nor the disaffection of the service [11], only temporary authorization for its administration.

Cases II and III do not have as focus a public concession or a privatization stricto sensu, but they do involve partnerships between private companies and the state to carry out fraud and security control.

As mentioned previously, the idea of smart cities is deeply associated with public-private partnerships [2]. The three cases mentioned in this study illustrate the presence of private agents in the development of smart cities, as shown in the items below.

3.1 Case I: Facial recognition for marketing purposes at Line 4 of the Sao Paulo subway system

In April 2018, Line 4 of the Sao Paulo subway announced the deployment of the so-called "Interactive Digital Doors" on some platforms [13].

According to the Brazilian Institute of Consumer Rights, which subsequently filed a class action against the company, the interactive doors had cameras and were located on the platforms used to board trains [13]. The collection of biometric data from users took place when they approached the platforms and operated using a facial recognition mechanism [13].

In this perspective, the doors would be able to identify the human presence, the number of people, and emotions. The goal of this technology was to capture the facial expressions of subway passengers in reaction to the advertisements available on the platform [12].

The lawsuit had as main arguments, among other issues, (i) the lack of information provided by the company, which did not detail the functioning of the doors nor did it properly inform users about the existence of such system and (ii) the illegality of the collection of biometric data without the consent and knowledge of citizens [13].

In September 2018, the Sao Paulo Court of Justice granted advance protection, determining the shutdown of the facial recognition system [13]. A resolution for the case is still pending a formal decision.

3.2 Case II: Facial recognition for fraud prevention in buses

In 2017, the state-owned company that manages the buses in the city of Sao Paulo installed facial recognition cameras in the entrance of buses circulating within the municipality to prevent fraud [16].

The adoption of this measure is due to the fact that, in the city of Sao Paulo, the elderly, students, and children are guaranteed by law the right to travel free of charge, or at a reduced rate on public transport. To acquire this right, beneficiary users register in the transport company and acquire an individual and non-transferable card, which works as a free or reduced-fare ticket for circulation in public transport.

The fraud detection system, therefore, would have as its main objective the identification of whether the person holding the transport card with free or reduced fare at the entrance of the bus is its legitimate holder [16].

Every time a passenger would go through the entrance of the bus, he/she would be submitted to an identity test that compares the images uploaded at the moment of the card’s registration with the live image of the person entering the bus and presenting that card. The images would then be compared to analyze if there is fraud [15].

When the system detects divergences with the registered photo, the user's transport card would be blocked and the user invited to provide clarifications. The installation of this system cost more than 74 million in Brazilian currency. Between 2017 and 2019, the City of Sao Paulo has blocked 331,641 cards for alleged fraud [16].

The Sao Paulo City Hall also confirms that this database is shared with other bodies when requested, such as the Military Police and the State Civil Police [16]. There is, however, verification by the state itself that the system has flaws and its fraud prevention analysis using facial recognition is not completely reliable, being still subject to numerous errors [17].

3.3 Case III: Bidding for facial recognition for security purposes on the São Paulo subway

In June 2019, the administrators of the subway of Sao Paulo announced a bidding notice for the creation of an electronic security monitoring system for the state-owned lines of the Sao Paulo subway. The amount foreseen in the bidding would be $ 58.6 million in Brazilian currency [18].

Among the technical requirements of the monitoring system presented in the announcement is facial recognition. According to the administrators of the Sao Paulo subway[1], the bidding sought to hire an experienced private company that had already implemented analogous technologies to improve its monitoring systems [14].

Some Brazilian civil society organizations filed a lawsuit against the initiative in 2020 [14]. According to the lawsuit, the company failed to perform its transparency duties, presenting incomplete and ambiguous information in response to requests for information made by Brazilian civil society [14].

The public notice released did not contain information about how the users' data will be collected and processed by the system, the databases that will be used as a reference for the system, the action protocols in case of identification of a possible suspect through the facial recognition system, the information security requirements used, and the initiatives to be taken to reduce the risk of data leaks [18].

In February 2020, the judge requested the service administrators to provide further evidence as requested by the organizations [14].

4. Citizens' privacy in the times of facial recognition in public services

In an objective light, the processing of biometric data consists of measuring and monitoring parts of the human body that allow for distinction between one person and the other [19].

Therefore, it is a sort of body coding in which the individual's biometric information is translated into binary language. Thus, people have a unique type of coded identity that represents them for access and recognition purposes [19].

With regard to facial recognition specifically, one of the factors that facilitate its massification as a monitoring apparatus in urban centers lies in the fact that the experience of having one's face recognized is close to imperceptible to the individual, who will hardly suffer any degree of physical discomfort by simply looking at a camera [19].

Thus, the use of sensors becomes so normal in urban spaces that they are "ubiquitous" and part of a daily routine that is imperceptible by the population [20] However, although it causes little physical discomfort, the processing of this type of information allows the

[1] This case refers to the subway lines that are managed by a state-owned company.

identification of extremely sensitive individualities about people, such as gender, race and health status.

The power of this type of technology, in addition to its subtlety and the increasing ubiquity that they acquire in people's lives, also resides in the ignorance of the potential network interactions that may derive from its operation [1].

Brazil has a data protection legislation approved in 2018 that emerges as a result of public consultations and multistakeholder participation and with strong influence from the GDPR. The law establishes a series of principles and legal grounds for data processing that should be applied to both the public and private sectors. The purpose of the principles is to guide all stages of data processing, in order to place limits on the use by the various agents involved and allow some control by the subject [21].

Compliance with the principles is also a requirement for the processing of data by the state, regardless of the legal nature of the entity that is in charge of the public service. These principles are based on provisions existing in different international frameworks, which are consolidated due to the fact that they are common to different international normative instruments, forming a kind of autonomous doctrine on the topic [21].

The cases addressed above bring up a series of issues involving some of the principles that guide data protection according to international standards which are incorporated by the Brazilian legislation. The principles that are relevant for this study and which will be analyzed in the following topics are: (i) transparency and accountability, (ii) purpose specification, use limitation and purpose compatibility, (iii) risk mitigation, harms and benefits assessment [22].

4.1 Accountability and transparency over personal data

The principles of transparency and accountability establish the need to provide clear and adequate information about the data processing so that the subject has the right to know the agents and mechanisms involved in the use of his/her personal information [22].

In light of the three cases analyzed in this study, there are explicit problems regarding transparency and accountability in two of them. Case I and III were the object of lawsuits and gaps in transparency were within the main complaints made regarding the implementation of the facial recognition initiatives.

Case I shows issues in the domain of transparency as the only public notification made regarding the facial recognition system was done through a brief note on the website [12].

In order to comply with this principle, it would be necessary for the company to have informed users about the implementation of the technology, its basic characteristics, and its purpose.

Case III also shows a similar scenario, as the public notice involving the contracting of a private company to implement facial recognition to improve security in the subway did not present essential information regarding the initiative. Besides this, the administrators of the subway system did not produce an impact assessment regarding the facial recognition technology, nor does it have studies that prove the safety of the databases to be used for the implementation of the system [14]

Thus, the cases show scenarios in which citizens, without complete knowledge, have their information processed by public and/or private actors without being notified about how this information will be used [19].

4.2 Surveillance as purpose deviation

Another issue is that the smart city necessarily creates the "smart citizen" and forces citizens to accept certain technologies in order to be included in social programs or participate in the civic life of the city [9]. That is, it does not give citizens the opportunity to choose whether or not they want to be part of databases involving facial recognition. In the cases mentioned, for instance, there is no alternative to use the public transport system without having one's facial expressions collected.

In the view of Hollands [4], this reduces the control structure in urban centers to a binary model divided between those that are included and, consequently, tacitly agree with the monitoring practices that surround them and the others, which are excluded from places and services.

This also highlights another discussion on the existence of a deviation from the original purpose of the public service provision itself. To which extent should a facial recognition service be considered essential to offering a public transportation system? This question is directly related to the discussion on purpose specification, use limitation, and compatibility.

The principle determines that data processing must be specific, compatible, or otherwise relevant, and not excessive in relation to the objective for which its access was obtained. This prohibits data from being collected with a purpose not linked with what motivated the beginning of the relationship with the data subject [22].

Case I involves the deployment of facial recognition aimed at monitoring people's reactions to advertisements. According to the responsible company's own declaration, it was aimed at "increasing sales" by identifying the facial reactions from users of the transportation system [12].

This monetization system by means of facial recognition presented in Case I, in turn, represents a clear deviation of purpose since it characterizes a departure from the strict administration of the transport service that caused the beginning of the relationship between the data controller and the citizen.

The principle also states that there must be compatibility between the purpose of data collection and the expectation of the data subject. This principle also carries with it the idea of informational self-determination, since it values the citizen’s perspective in relation to the use of his/her information [21].

In the specific case, there is an issue involving compliance with the principle, since the users of the service, when walking on the platforms, have as their primary objective that of being transported between stations, without any expectation of having their facial expressions captured for the purpose of publicity.

According to international standards, the processing of personal data must be restricted to the minimum necessary for the provision of the service [22]. Since the party is a public service provider, the collection of information should be restricted to the minimum necessary for the provision of this service, so that the excessive use of data would be characterized as non-compliant with international standards on the principles of privacy and data protection.

When looking at Cases II and III, similar issues involving the purposes of facial recognition arise. In what circumstances should citizens have their faces exposed to facial recognition?

The purpose is easily questionable when looking at initiatives such as those adopted in both cases. What kind of practice do these cameras aim to combat or encourage? Why is combating fraud in the gratuity of the transport seen as essential to the transport service? There are other passengers who are not beneficiaries of the gratuity or fare reduction benefits, and because the cameras are at the entrance of the buses, these passengers are also subject to collection of their biometric data, even though the monitoring of fraud does not apply to them.

4.3 The risks of biometric-based automated law enforcement

Both the state and the private sector are dependent on mechanisms for identifying citizens. Within this context, the growth in the use of biometric information for the identification of people is part of a general trend towards identity and authenticity verification rituals [9].

This trend leads to the integration of security tools dependent on surveillance devices. In this sense, automated law enforcement systems are essentially characterized by the use of mechanisms of surveillance, and aggregation of information to identify individuals acting contrary to the law [20].

The idea of smart cities, in this way, is accompanied by initiatives aimed at the establishment of devices that sophisticate control and monitoring mechanisms by governments and the private sector and restrict the sphere of freedoms granted to citizens

[1]. The official discourse that supports this type of initiative is that some freedoms must be sacrificed in the name of security [23].

The application of technology to police power and law enforcement is, of course, not a consequence of smart cities, but these, in turn, have a great potential to intensify them [1]. The development of technologies such as facial recognition and its application in the context of public services illustrate the sophistication of surveillance devices under the justification of preventing illicit conduct.

These technologies that associate biometric data to conduct control are symptomatic of an even deeper social development in which the fusion between the body and technology becomes part of contemporary governance models and integrates automated law enforcement systems [9].

This is because bodies serve as a kind of "token" that we carry with us all the time, which makes the task of avoiding facial recognition technologies difficult [9]. Given this characteristic, biometric identification becomes progressively used as a mechanism for access control [9].

Case II and III and the implementation of facial recognition applied to the subway and bus systems in the city of Sao Paulo illustrate this paradigm perfectly, since the main objectives of such initiatives are to monitor the entry and exit of passengers from the buses and stations in order to detect possible fraud and improve security.

Another key feature of these systems is their ability to process and analyze information at speeds greater than human capabilities through algorithmic solutions [20]. Automated law enforcement thus represents a type of innovation in public governance that has code as the center of its operation [20]. When merged with the use biometric identification, these automatized methods of conduct control represent an evolution of monitoring to a level of access control and behaviors molded basically on the body.

Foucault addresses this intersection between the body and the machine when defining the concept of “biopower”, in which the body of individuals is integrated into control systems and it becomes possible to analyze it and restrict its liberty using machine-based control [24].

In this scenario, the city is no longer an organic organism whose production of information occurs spontaneously and dispersed. It then becomes controllable by logical and rational decisions taken through algorithmic governance mechanisms [2].

However, this makes citizens subject to decisions that present numerous ethical risks. These risks lie in the very nature of the technology and the conflicts derived from the delegation of essentially human functions to it. This stems from the fact that code requires a high degree of precision and objectivity, while legal text is highly abstract and subject to interpretation, summed with the fact that the activity of police power is dependent on analysis and interpretations that are traditionally designed to be performed by humans [20].

Surveillance applied to the body becomes a form of “social sorting” carried out by non-human entities [9]. It is foreseeable, therefore, that facial recognition is considered to be quite susceptible to racial discrimination and other undesirable biases. In general, the foundations on which these technologies are structured are not entirely reliable, as it is not uncommon for them to be inaccurate, incomplete, or used completely out of context [25].

Systems of this nature are always subject to false positives and false negatives. Ideally, if an individual does not commit a crime, he/she is not accused of committing it, but a facial recognition system can cause a false positive in which the subject is considered suspect and may have restricted rights that would be originally legitimate [20]. In a society in which police power is delegated to algorithmic entities, individuals lose the right to individualized treatment, as people are reduced to nodes in a control network [1].

Surveillance and automated law enforcement are also generally not designed to allow facilitated access to due process [23]. These automated control processes are unlikely to have any mechanism that allows for effective means by which individuals can correct, contextualize, or oppose the information that is used against them in time to not have their rights restricted.

The increase in the use of automated surveillance mechanisms, therefore, poses a risk of dehumanizing the public governance process. It can be considered a reductionist and functionalist approach to urban governance that leads to control of conduct and risk elimination that does not take into account human factors involved in urban governance [2].

The objective of exposing citizens to constant surveillance ends up promoting self-discipline [23]. The rationalized and often apolitical discourse around the use of technology for control of illegal activity in order to make urban environments “disciplined” has the potential to reduce phenomena such as politics, conflicts, insurgency, and resistance, which are a natural part of urban life [9].

This type of technology can cause a chilling effect on civil rights such as freedom of association, assembly, and expression. Surveillance distorts the relationship between citizens and police power, creating an asymmetry of knowledge and power. In addition, the speed with which technological advances allow intrusion into citizens' lives is not accompanied by regulatory efforts to ensure that rights are not violated [23].

5. Conclusion

The term smart cities has been increasingly used to designate an idea of technological innovation as a path towards solving social problems present in urban contexts.

However, the very concept of a smart city is optimistic and generic and no precise definition is currently found to this term [9]. The discourse around smart cities is closely linked to political and economic actors for the formulation of specific development policies that are motivated by market interests [9].

The deployment of facial recognition initiatives in the Sao Paulo transportation system is an example of the application of surveillance technologies in the context of urban public services, an increasingly evident trend deeply inserted into the context of smart cities.

In the cases under analysis, biometric data is compulsorily collected with dubious transparency mechanisms and for purposes whose direct relation with the offering of public transportation is questionable.

Moreover, facial recognition can offer huge dangers to privacy. In this sense, the implementation of this type of initiative is an evident risk of loss, by citizens, of some of their freedoms, being subject to constant practices of monitoring and conduct control.

Through the analysis of the conformity of the conduct in relation to the principles that govern data protection at the international level and also at the national level, it is possible to observe, therefore, a trend towards a collision between the practices carried out by the state in the three cases analyzed.

Acknowledgments

A special thanks to Anna Campanelli and Maíra Campanelli for their help with revision and formatting.

References

[1] Pasquale, F., & Sadowski, J (2015). The spectrum of control: A social theory of the smart city. First Monday. https://doi.org/10.5210/fm.v20i7.5903

[2] Kitchin, R. (2013). The Real-Time City? Big Data and Smart Urbanism. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2289141

[3] Hollands, R. G. (2008). Will the real smart city please stand up?: Intelligent, progressive or entrepreneurial? City, 12(3), 303–320.

[4] Klauser, F., Paasche, T., & Söderström, O. (2014). Smart cities as corporate storytelling. City, 18(3), 307–320. https://doi.org/10.1080/13604813.2014.906716

[5] Anderson, A. L. & Cooke, C. D.(2017). Autonomous Radios and Open Spectrum in Smart Cities. In H. Song, R. Srinivasan, T. Sookoor, & S. Jeschke (Eds.), Smart Cities (pp. 99–123). John Wiley & Sons, Inc. https://doi.org/10.1002/9781119226444.ch4

[6] Kumar, S. A. P. & Raj, P.(2017). Big Data Analytics Processes and Platforms Facilitating Smart Cities. In H. Song, R. Srinivasan, T. Sookoor, & S. Jeschke (Eds.), Smart Cities (pp. 23–52). John Wiley & Sons, Inc. https://doi.org/10.1002/9781119226444.ch2

[7] Jameson, S., Perez de Pulgar, C., Richter, C., Taylor, L. (2016). Customers, Users or Citizens? Inclusion, Spatial Data and Governance in the Smart City (SSRN Scholarly Paper ID 2792565). Social Science Research Network. https://papers.ssrn.com/abstract=2792565

[8] Shelton, T.,Wiig, A., & Zook, M.(2015). The 'actually existing smart city.' Cambridge Journal of Regions, Economy and Society, 8(1), 13–25. https://doi.org/10.1093/cjres/rsu026

[9] Vanolo, A. (2014). Smartmentality: The Smart City as Disciplinary Strategy. Urban Studies, 51(5), 883–898. https://doi.org/10.1177/0042098013494427

[10] Souto, M. J. V. (2003). Direito Administrativo da Economia. Direito Administrativo da Economia. Lumen Juris.

[11] Mello, C. A. (2016). Curso de Direito Administrativo (37th ed.). Malheiros.

[12] Meier, R. (2018, April 16). Portas de plataforma da Linha 4-Amarela vão "interpretar" suas reações. Metrô CPTM. https://www.metrocptm.com.br/portas-de-plataforma-da-linha-4-amarela-vao-interpretar-suas-reacoes/

[13] Instituto de Defesa do Consumidor v. ViaQuatro (2018). Processo n. 1090663-42.2018.8.26.0100. Tribunal de Justiça do Estado de São Paulo.

[14] Defensoria Pública do Estado de São Paulo v. Metrô de São Paulo (2020). Processo n. 1006616-14.2020.8.26.0053. Tribunal de Justiça do Estado de São Paulo.

[15] Zvarick, L. (2019, June 12). Reconhecimento facial bloqueia 331 mil Bilhetes Únicos em SP. Folha de São Paulo. https://agora.folha.uol.com.br/sao-paulo/2019/06/reconhecimento-facial-bloqueia-331-mil-bilhetes-unicos-em-sp.shtml

[16] Payão, F. (2019, June 12). São Paulo bloqueia 331 mil Bilhetes Únicos após reconhecimento facial. Tecmundo. https://www.tecmundo.com.br/seguranca/142472-paulo-bloqueia-331-mil-bilhetes-unicos-reconhecimentofacial.htm#:~:text=A%20SPTrans%2C%20respons%C3%A1vel%20pelos%20%C3%B4nibus,para%20buscar%20algum%20poss%C3%ADvel%20problema.&text=O%20banco%20de%20dados%20da%20prefeitura%20%C3%A9%20alimentado%20diariamente.

[17] Secretaria Municipal de Mobilidade e Transportes (SMT). (2019). Relatório de Auditoria (008/2019/CGM-AUDI). Controladoria Geral do município. https://www.prefeitura.sp.gov.br/cidade/secretarias/upload/controladoria_geral/RF_008_2019___VFinal_SPTrans_24_03_2020.pdf

[18] Sakamoto, L.(2020, June 2). Ação exige que Metrô explique licitação milionária de reconhecimento facial. Uol Notícias. https://noticias.uol.com.br/colunas/leonardo-sakamoto/2020/02/12/acao-exige-que-metro-explique-licitacao-milionaria-de-reconhecimento-facial.htm

[19] Aas, K. F. (2016). 'The body does not lie': Identity, risk and trust in technoculture: Crime, Media, Culture. https://doi.org/10.1177/1741659006065401

[20] Conti, G., Hartzog, W., Larkin, D., Nelson, J., Shay, L. A.(2016). Confronting automated law enforcement. Robot Law. https://www.elgaronline.com/view/edcoll/9781783476725/9781783476725.00019.xml

[21] Doneda, D. (2015b). Princípios e proteção de dados pessoais., Direito & Internet III. Marco Civil da Internet - Tomo I (1st ed., Vol. 3, pp. 369–370). Quartier Latin.

[22] United Nations. (2017). UNSDG | Data Privacy, Ethics and Protection: Guidance Note on Big Data for Achievement of the 2030 Agenda. United Nations. https://unsdg.un.org/resources/data-privacy-ethics-and-protection-guidance-note-big-data-achievement-2030-agenda

[23] Fox, R. (2016). Someone to Watch Over Us:: Back to the Panopticon? Criminal Justice. https://doi.org/10.1177/1466802501001003001

[24] Peggs, K., & Smart, B. (2018). Foucault's Biopower. In L. Downing (Ed.), After Foucault: Culture, Theory, and Criticism in the 21st Century (pp. 61–76). Cambridge University Press. https://doi.org/10.1017/9781316492864.006

[25] O'Neil, C. (2016). Weapons of math destruction: how big data increases inequality and threatens democracy (First edition). Crown.